

WHAT IS CLAIMED IS:

- 1 1. A method of establishing a secure communication path
2 between a computer system and a remote computer system
3 comprising:
4 exchanging identification data with the remote
5 computer system using a communication path;
6 determining, based on the identification data, whether
7 a predefined security policy exists corresponding
8 to the remote computer system; and
9 establishing a secure communication path using a
10 default security policy in response to
11 determining that the predefined security policy
12 does not exist.
- 1 2. The method as described in claim 1 wherein the
2 identification data is selected from the group
3 consisting of a gateway address, a host name, a user
4 identifier, an IP address, and a distinguished name.
- 1 3. The method as described in claim 1 wherein
2 establishing the secure communication path further
3 includes:
4 determining whether a digital certificate or a pre-
5 shared key is used for encrypting data.
- 6 4. The method as described in claim 1 further comprising:
7 searching a group table for a group identifier
8 corresponding to the remote computer system;
9 wherein the predefined security policy corresponds to
10 the group identifier in response to a successful
11 group identifier search.

1 5. The method as described in claim 1 further comprising:
2 selecting a proposal and transforms corresponding to
3 the default security policy;
4 creating a security association payload using the
5 selected proposal and transforms; and
6 sending the security association from one computer
7 system to the remote computer system.

1 6. The method as described in claim 5 further comprising:
2 receiving a response from the remote computer system;
3 determining whether the proposal was accepted by the
4 other computer system; and
5 verifying identification information in response to
6 the proposal being accepted.

1 7. The method as described in claim 1 further comprising:
2 verifying a remote identifier and a digital signature
3 corresponding to the remote computer system; and
4 creating the secure communication path to the remote
5 computer system in response to the verification.

1 8. An information handling system comprising:
2 one or more processors;
3 a memory accessible by the processors;
4 a nonvolatile storage accessible by the processors;
5 a network interface connecting the information
6 handling system to a computer network; and
7 a network tool for creating a secure communication
8 path to a remote computer system, the network
9 tool including:

10 means for exchanging identification data with the
11 remote computer system using a communication
12 path;
13 means for determining, based on the
14 identification data, whether a predefined
15 security policy exists corresponding to the
16 remote computer system; and
17 means for establishing a secure communication
18 path using a default security policy in
19 response to determining that the predefined
20 security policy does not exist.

1 9. The information handling system as described in claim
2 8 wherein the identification data is selected from the
3 group consisting of a gateway address, a host name, a
4 user identifier, an IP address, and a distinguished
5 name.

1 10. The information handling system as described in claim
2 8 wherein the means for establishing the secure
3 communication path further includes:
4 means for determining whether a digital certificate or
5 a pre-shared key is used for encrypting data.

6 11. The information handling system as described in claim
7 8 further comprising:
8 means for searching a group table for a group
9 identifier corresponding to the remote computer
10 system;
11 wherein the predefined security policy corresponds to
12 the group identifier in response to a successful
13 group identifier search.

1 12. The information handling system as described in claim
2 8 further comprising:

3 means for selecting a proposal and transforms

4 corresponding to the default security policy;

5 means for creating a security association payload

6 using the selected proposal and transforms; and

7 means for sending the security association from one

8 computer system to the remote computer system.

1 13. The information handling system as described in claim
2 12 further comprising:

3 means for receiving a response from the remote

4 computer system;

5 means for determining whether the proposal was

6 accepted by the other computer system; and

7 means for verifying identification information in

8 response to the proposal being accepted.

1 14. A computer program product stored on a computer
2 operable medium for establishing a secure
3 communication path between a computer system and a
4 remote computer system comprising:

5 means for exchanging identification data with the

6 remote computer system using a communication

7 path;

8 means for determining, based on the identification

9 data, whether a predefined security policy exists

10 corresponding to the remote computer system; and

11 means for establishing a secure communication path

12 using a default security policy in response to

13 determining that the predefined security policy

14 does not exist.

1 15. The computer program product as described in claim 14
2 wherein the identification data is selected from the
3 group consisting of a gateway address, a host name, a
4 user identifier, an IP address, and a distinguished
5 name.

1 16. The computer program product as described in claim 14
2 wherein the means for establishing the secure
3 communication path further includes:
4 means for determining whether a digital certificate or
5 a pre-shared key is used for encrypting data.

6 17. The computer program product as described in claim 14
7 further comprising:
8 means for searching a group table for a group
9 identifier corresponding to the remote computer
10 system;
11 wherein the predefined security policy corresponds to
12 the group identifier in response to a successful
13 group identifier search.

1 18. The computer program product as described in claim 14
2 further comprising:
3 means for selecting a proposal and transforms
4 corresponding to the default security policy;
5 means for creating a security association payload
6 using the selected proposal and transforms; and
7 means for sending the security association from one
8 computer system to the remote computer system.

1 19. The computer program product as described in claim 5
2 further comprising:

3 means for receiving a response from the remote
4 computer system;

5 means for determining whether the proposal was
6 accepted by the other computer system; and

7 means for verifying identification information in
8 response to the proposal being accepted.

1 20. The computer program product as described in claim 14
2 further comprising:

3 means for verifying a remote identifier and a digital
4 signature corresponding to the remote computer
5 system; and

6 means for creating the secure communication path to
7 the remote computer system in response to the
8 verification.

1